Exhibit A

US005845070A

United States Patent [19]

Ikudome

[11] **Patent Number: 5,845,070**

[45] **Date of Patent: Dec. 1, 1998**

[54] **SECURITY SYSTEM FOR INTERNET PROVIDER TRANSACTION**

[75] Inventor: **Koichiro Ikudome**, Arcadia, Calif.

[73] Assignee: **Auric Web Systems, Inc.**, Pasadena, Calif.

[21] Appl. No.: **769,590**

[22] Filed: **Dec. 18, 1996**

[51] **Int. Cl.**^{6} **G06F 11/00**

[52] **U.S. Cl.** **395/187.01**; 395/186; 395/187.01; 395/188.01; 395/200.59; 380/25

[58] **Field of Search** 395/200.16, 200.17, 395/187.01, 186, 188.01, 200.59; 380/25

[56] **References Cited**

U.S. PATENT DOCUMENTS

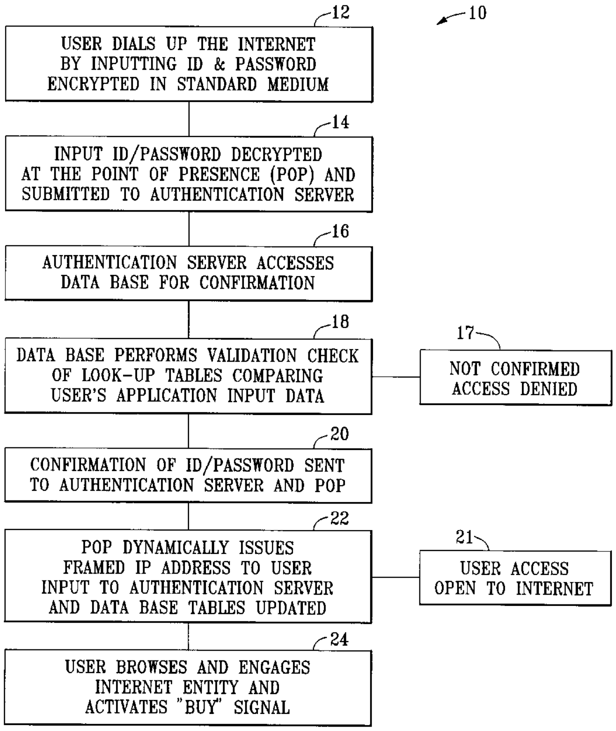
4,218,738	8/1980	Matyas et al.	380/25
5,694,595	12/1997	Jacobs et al.	395/187.01
5,696,898	12/1997	Baker et al.	395/187.01
5,699,513	12/1997	Feigen et al.	395/187.01

Primary Examiner—Robert W. Beausoliel, Jr.
Assistant Examiner—Pierre Eddy Elisca
Attorney, Agent, or Firm—Sheldon & Mak

[57] **ABSTRACT**

This invention provides security controls against exposing Confidential Information that is required to purchase goods and services from Internet Entity **56** offered on a home page site. The Confidential Information is input to a data base **52** which is part of a tracking and authentication module **50**. Including in the tracking and authentication module **50** is a certification server **54**, and authentication server **53** and the data base **52**. A series of look-up tables, 200, 300 and 400 are provided in the data base **52** and the data entries in the tables, including the Confidential Information, is tied to a first data set which typically includes a user's ID/password and a second data set comprising a framed IP address issued for use only during each log-in - log-out session. It can be any form of alpha-numerical designation. The Confidential Information contained in table 400, if misappropriated, could be used to make purchases chargeable to the user. The purchases can be made without the Confidential Information leaving the data base **52** (table 400). The second data set is used to query the module **50** for validation of the user's creditworthiness and transaction completed by the data base sending a message to the issuer of the credit card to charge the user's account or alternatively noticing the Internet Entity to directly bill user. An additional security measure is provided by the system assigning a third data set consisting of the destination address of each and every Internet Entity that the user contacts during a log-in - log-out session which is tracked by being entered into any one of the tables 200, 300 or 400. It provides another level of validation against the first and second data sets.

13 Claims, 4 Drawing Sheets


10
12
USER DIALS UP THE INTERNET BY INPUTTING ID & PASSWORD ENCRYPTED IN STANDARD MEDIUM
14
INPUT ID/PASSWORD DECRYPTED AT THE POINT OF PRESENCE (POP) AND SUBMITTED TO AUTHENTICATION SERVER
16
AUTHENTICATION SERVER ACCESSES DATA BASE FOR CONFIRMATION
18
DATA BASE PERFORMS VALIDATION CHECK OF LOOK-UP TABLES COMPARING USER'S APPLICATION INPUT DATA
17
NOT CONFIRMED ACCESS DENIED
20
CONFIRMATION OF ID/PASSWORD SENT TO AUTHENTICATION SERVER AND POP
22
POP DYNAMICALLY ISSUES FRAMED IP ADDRESS TO USER INPUT TO AUTHENTICATION SERVER AND DATA BASE TABLES UPDATED
21
USER ACCESS OPEN TO INTERNET
24
USER BROWSES AND ENGAGES INTERNET ENTITY AND ACTIVATES "BUY" SIGNAL

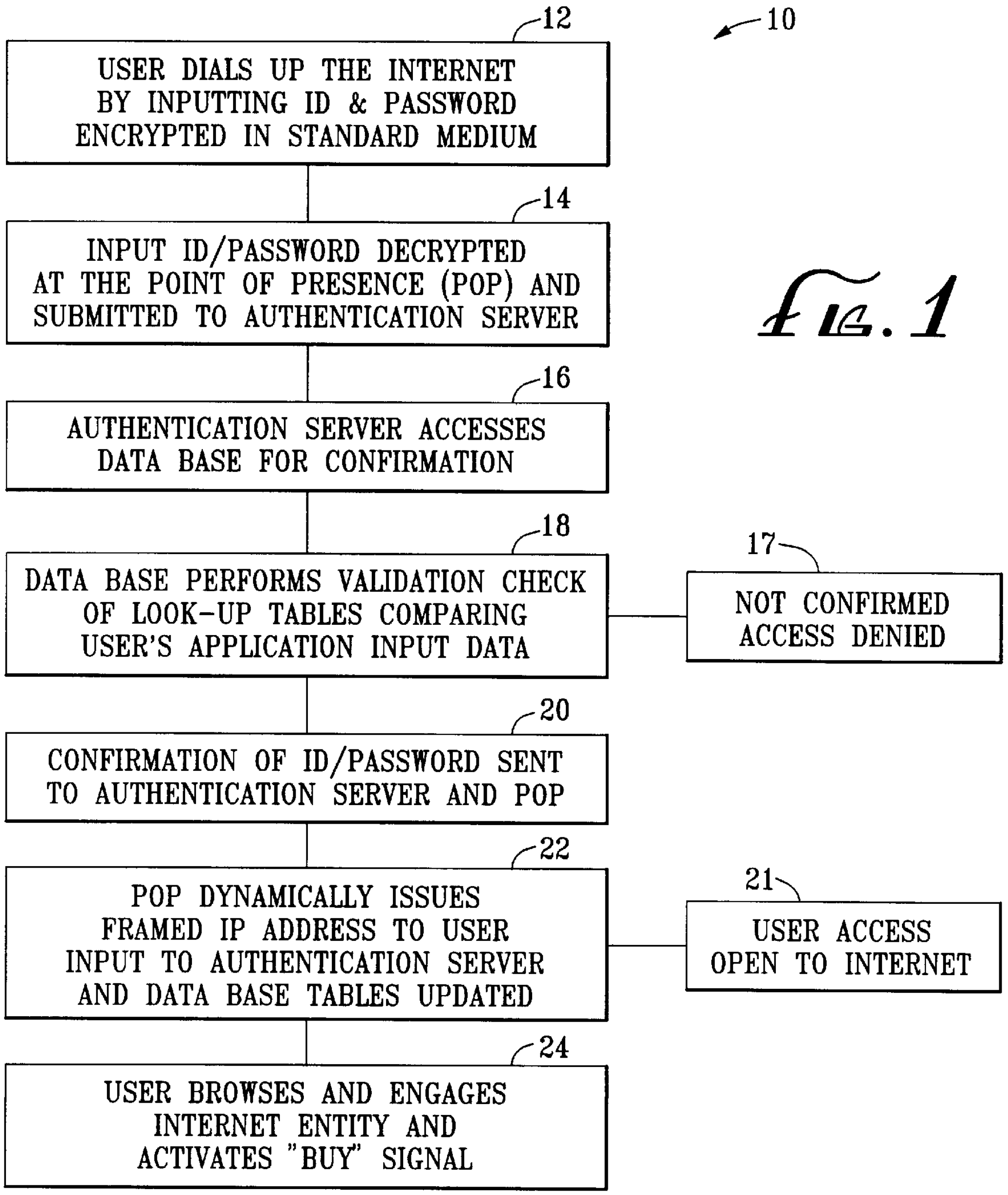

10
12
USER DIALS UP THE INTERNET BY INPUTTING ID & PASSWORD ENCRYPTED IN STANDARD MEDIUM
14
INPUT ID/PASSWORD DECRYPTED AT THE POINT OF PRESENCE (POP) AND SUBMITTED TO AUTHENTICATION SERVER
16
AUTHENTICATION SERVER ACCESSES DATA BASE FOR CONFIRMATION
18
DATA BASE PERFORMS VALIDATION CHECK OF LOOK-UP TABLES COMPARING USER'S APPLICATION INPUT DATA
17
NOT CONFIRMED ACCESS DENIED
20
CONFIRMATION OF ID/PASSWORD SENT TO AUTHENTICATION SERVER AND POP
22
POP DYNAMICALLY ISSUES FRAMED IP ADDRESS TO USER INPUT TO AUTHENTICATION SERVER AND DATA BASE TABLES UPDATED
21
USER ACCESS OPEN TO INTERNET
24
USER BROWSES AND ENGAGES INTERNET ENTITY AND ACTIVATES "BUY" SIGNAL

FIG. 1

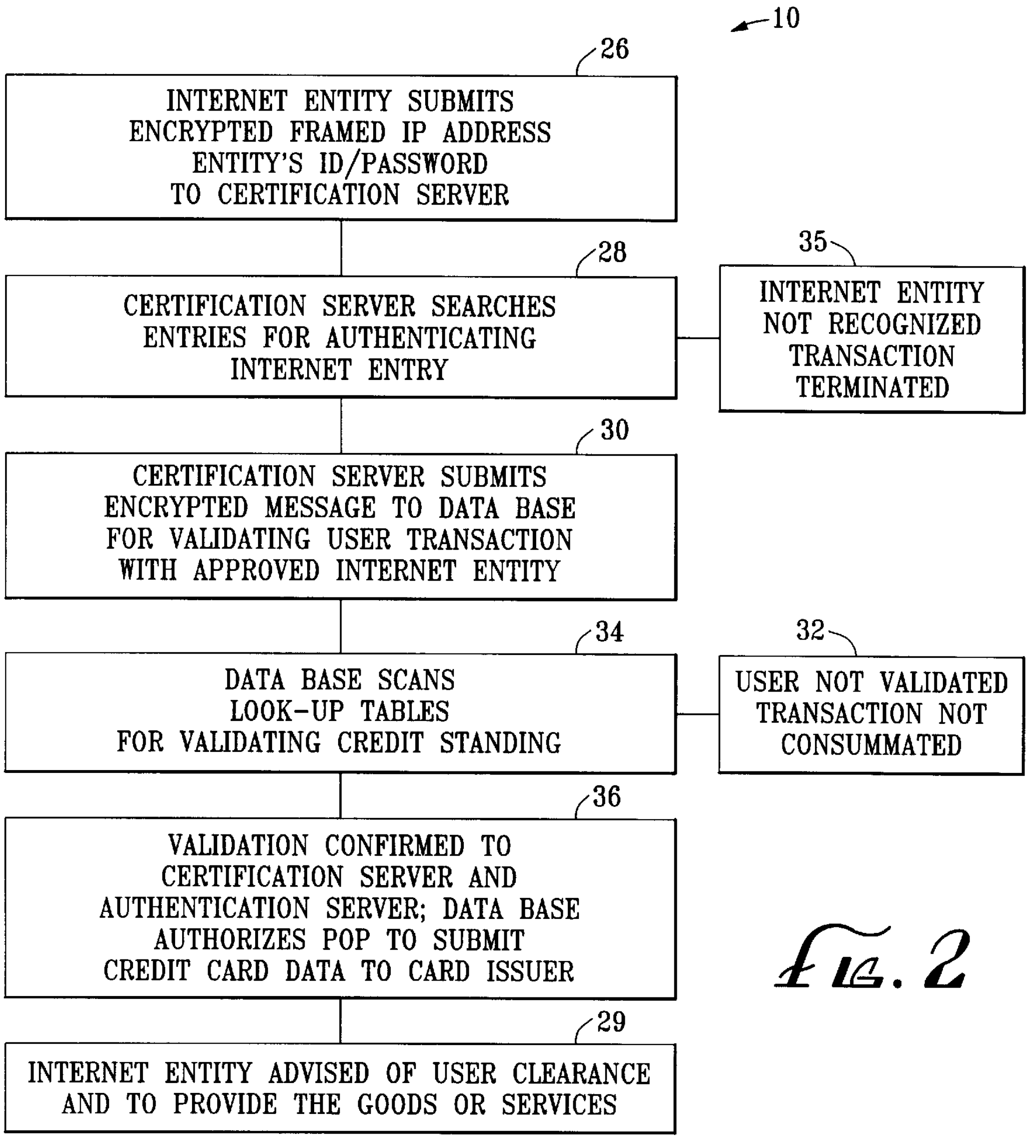

10
26
INTERNET ENTITY SUBMITS ENCRYPTED FRAMED IP ADDRESS ENTITY'S ID/PASSWORD TO CERTIFICATION SERVER
28
CERTIFICATION SERVER SEARCHES ENTRIES FOR AUTHENTICATING INTERNET ENTRY
35
INTERNET ENTITY NOT RECOGNIZED TRANSACTION TERMINATED
30
CERTIFICATION SERVER SUBMITS ENCRYPTED MESSAGE TO DATA BASE FOR VALIDATING USER TRANSACTION WITH APPROVED INTERNET ENTITY
34
DATA BASE SCANS LOOK-UP TABLES FOR VALIDATING CREDIT STANDING
32
USER NOT VALIDATED TRANSACTION NOT CONSUMMATED
36
VALIDATION CONFIRMED TO CERTIFICATION SERVER AND AUTHENTICATION SERVER; DATA BASE AUTHORIZES POP TO SUBMIT CREDIT CARD DATA TO CARD ISSUER
29
INTERNET ENTITY ADVISED OF USER CLEARANCE AND TO PROVIDE THE GOODS OR SERVICES

FIG. 2

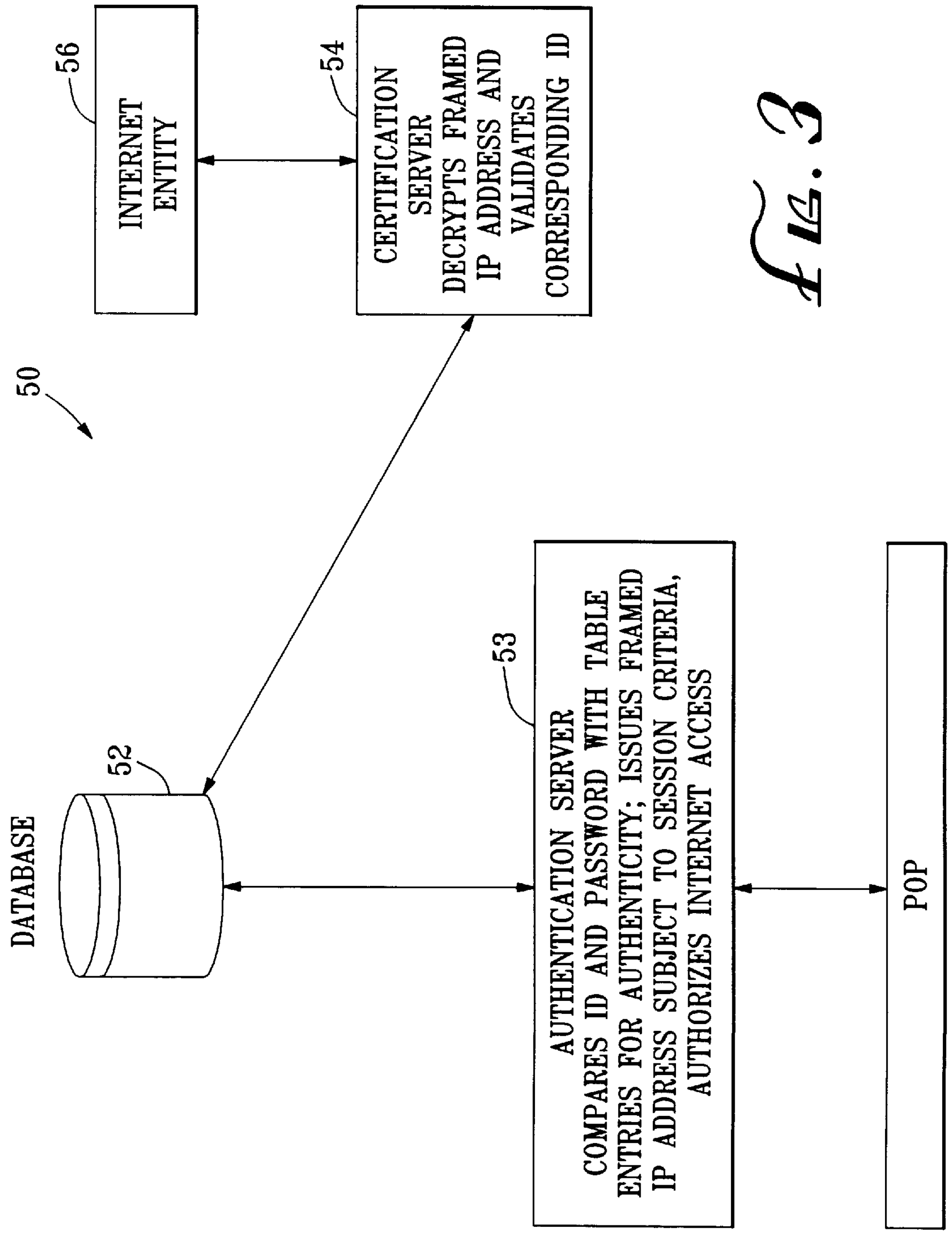

50
56
INTERNET ENTITY
54
CERTIFICATION SERVER DECRYPTS FRAMED IP ADDRESS AND VALIDATES CORRESPONDING ID
DATABASE
52
53
AUTHENTICATION SERVER COMPARES ID AND PASSWORD WITH TABLE ENTRIES FOR AUTHENTICITY; ISSUES FRAMED IP ADDRESS SUBJECT TO SESSION CRITERIA, AUTHORIZES INTERNET ACCESS
POP

Fig. 3

TABLES:

100

ASSIGNED_IP_ADDRESS

200

IP_ADDRESS	USER_ID	DESTINATION ADDRESS

SESSION_TABLE

300

SESSION_ID	USER_ID	LOGIN_TIME	LOGOUT_TIME	

USER_TABLE

400

USER_ID	PASSWORD	AMOUNT_USED	AMOUNT_LIMIT	CREDIT CARD NO.	CREDIT LIMIT	CREDIT RATING	DRIVER'S LICENSE NO	

FIG. 4

SECURITY SYSTEM FOR INTERNET PROVIDER TRANSACTION

BACKGROUND

This invention relates generally to a method of authenticating an Internet user's identity and providing security control for confidential information usable for completing transactions with an Internet Entity and more particularly to the preservation and tracking of the flow of confidential information necessary to complete the transaction during a specific log-in - log-out session on the Internet.

DISCUSSION

The advent of the Internet System has generated a growing number of individuals subscribing to the services of an Internet Service Provider desirous of purchasing goods or other services. Usually a user will access the system by inputting some personal identification and a password. While the ability to simply access the system by dialing up using a PC is a desirable feature, it exposes the user to the risk of having its confidential information misappropriated. Usually, a user as part of the subscription application will disclose to the Internet provider necessary credit card information, credit ratings, driver's license information, credit limits, a social security number and other pertinent information (all hereinafter referred to as "Confidential Information") which could be misappropriated and any resulting unauthorized use cause financial loss to the user.

A number of methods have been proposed to provide security for the kinds of Confidential Information that is typically exchanged between a user and an Internet Entity. For example, such systems bearing the trade names CYBERCASH and NETCASH are currently available. Such known systems suffer from the disadvantage that the user is required to provide the software to encrypt the protected information. It will be understood that any encrypted message requires appropriate decryption software available to the Internet Entity who is a party to the transaction.

Currently, a user can access the Internet by providing an identification number and/or password which forms the basis for entry to the system. Generally, the Transport Control Protocol (TCP) used in Internet communications, in conjunction with Internet Protocol (IP) offers some measure of security because the unauthorized use of the IP address would be readily recognized by the TCP thereby thwarting the unauthorized use. Presently available dial-up services will accept a user's personal identification number (ID) or other identifying password to bridge a proprietary communication line with Internet. Using well known point of presence (POP) the ID is submitted to an authentication server to check whether the ID is in the authentication server protocol database. Authentication will result in the POP issuing a pre-assigned framed user IP address. Thus the user is assigned a framed IP address in accordance with known systems but there is absent any control relating it to the user's Confidential Information. The issuance of the framed IP address is a gating function that identifies the user as a subscriber and any additional data entered into the system merely courses through unprotected. Prior to completing any transaction the Internet Entity will request clearance of user's Confidential Information. This is where the currently known security controls fail to protect the user's Confidential Information against potential misappropriation and unauthorized use.

SUMMARY OF THE INVENTION

The invention provides a method for authenticating a user's Confidential Information and preserving it against unauthorized use when carrying out a transaction on the Internet. The security feature of the invention involves establishing a database to which is input the user's assigned framed IP address which becomes the second data set valid only for a specific log-in - log-out session. As part of this security feature, there is provided a tracking and authentication module comprising a certification server, an authentication server and a database each performing a validation function before authorizing use of the user's Confidential Information stored in the database.

The security process is initiated when the user logs onto the Internet using an ID and a password which represents a first data set. As the user selects an Internet Entity with which it intends to carry out a transaction, such as for example, a purchase transaction to be paid by credit card or the issuance of a billing statement, the first set of data is fed into a computer base controller to control modems and communication protocols (PPP) running on an equipment known as point of presence (POP) subject to a security key. As part of the security feature, the database will have input the necessary Confidential Information of the user as part of the subscription process. The first data set is tied to the Confidential Information. The POP transmits the first data set to the authentication server of the tracking and authentication module requesting validation. The authentication server in turn accesses the data base which includes a series of look-up tables enabling a comparison of the first data set with the Confidential Information. In response to a database check of the user ID, the authentication server authorizes the POP to issue in real time a new framed IP address. To effect a transaction with an Internet Entity the user keys in an appropriate signal which is a "buy" order. The buy order signal initiates the transaction by passing the second data set to the Internet Entity which starts the validation process through the tracking and authentication module.

The authentication server, reading a successful match will communicate with the POP identifying the assigned framed IP address to the user. Concurrently the framed IP address is input to the database updating the look-up tables. The third component of the tracking and authentication module is the certification server which is accessed by the Internet Entity, e.g. an Internet home page site. Based on the second data set, the framed IP address, a transaction between a user and the Internet Entity is screened by the Entity submitting the framed IP address to the certification server. There is provided in the certification server validation data that authenticates the Internet Entity as authorized to offer its services on the Internet. After an initial authentication of the Internet Entity, the user's framed IP address is input to the database for a match with the look-up tables.

The database in response to a user ID inquiry determines the identity of the user that is currently using the framed IP address, tieing the Confidential Information corresponding to the user ID. The data base will record the charges for the transaction and send a billing statement or instruct the certification server to release the Confidential Information to the Internet Entity through data encryption. In special circumstances the data base will authorize the credit card issuer to charge user's account.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. **1** and **2** show a flow chart of the method of dynamically authenticating a user and assigning a framed IP address to the user in accordance with the principles of this invention;

FIG. **3** shows the relationship of the tracking and authentication modules of this invention;

FIG. **4** shows the representative data in the look-up tables in the data base of FIG. **2**; and

Appendices A-1, A-2 and A-3 of the software listings.

DETAILED DESCRIPTION

Referring to FIGS. **1** through **4**, they show the general method of the invention identified with the general reference numeral **10**. It provides for authenticating a user to conduct transactions on the Internet during a specific log-in - log-out session and provides appropriate security control of the Confidential Information necessary to complete the transaction. Reference will also be made to the relevant numbered items in the software listing of Appendices A-1, A-2 and A-3.

Typically the user will access the Internet from a personal computer (PC) by inputting his identification and password as a first data set **12**. The first data set is sent to an authentication server **14** where it is subjected to a first validation check **16** and submitted to the database tables (FIG. **4**), identified generally with the reference numeral corresponding to lines 2 and 3 in Appendix A-3. Confirmation of the initial validation check **18** (FIG. **1**) of the first data set will generate a second data set **20** and **22**. As will be understood the validation certification and authentication processes are carried out in real time. The dynamically assigned framed IP address to new user is a known function of the POP. It will be appreciated that the second data set can comprise any form of alpha or numeric data and it is intended that it not be limited to an address form.

The tracking and authentication module (FIG. **3**) of this invention, identified generally with the numeral **50**, significantly expands the protection beyond the initial issuance of the new framed IP address. With the validation of the user's ID/password (first data set) and issuance of the second data set (**20** and **22**) the framed IP address, the POP has initiated the log-in process for the user. Accompanying the log-in message is such information as the time record, ID and framed IP address. These are entered into the tables, 200 and 300, shown in FIG. **4** Software listing: A-1: 37, 41, A-2: 113, 117. The database of FIG. **3** is expanded to contain the previously submitted Confidential Information that corresponds to the user's first data set (ID/password) and second data set (framed IP address). By these data base entries the user's Confidential Information is tied to the first and second data sets.

Included in the data requirements for the database is a destination address. It will be understood that the tracking and authentication module **50** can perform its security control using only the framed IP address. However, when combined with the destination address which is the IP address of the Internet Entity it affords an additional level of security. The user is issued the framed IP address **20** and **22** and can use it for the instant transaction with an Internet Entity to purchase either goods or services.

FIG. **3** illustrates the software that comprises the tracking and authentication module identified generally with the numeral **50**. It is effective in controlling the confidentiality of the user's information. Included in the tracking and authentication module **50** is the data base **52**, the authentication server **53** and the certification server **54**. The Internet Entity **56** is equipped with software that communicates with the certification server **54**. The user's Confidential Information is made part of the data base **52** at the time it subscribes to use the Internet. The data base **52** software includes a server of look-up tables which contain the user's Confidential Information as shown in FIG. **4**. As a user initiates access to the Internet by inputting its first data set **12** to the point of presence (POP) it is submitted to the authentication server **53** where it is run through a check to match it to the user's ID and password, table 400 referenced in Appendix A-3: 2, 3. The log-in time will be input to the table **300**. Upon finding a match the authentication server **53** sends a validation message to the POP referenced in Appendix A-2: 120, 121, issues a second data set, namely a new framed IP address which concurrently updates the data base **52** in accordance with Appendix A-1: 37, 41 with corresponding user ID.

The user thereafter will refer to the framed IP address as he surfs through the various Internet Entities looking for particular goods or services during a log in session. As the user engages Internet Entities using his framed IP address the tracking and authentication module **50** will access the certification server **54** validating the Internet Entity authenticating the user by his framed IP address.

The Internet Entity which is also known as the world wide web server (WWW) is represented by the certification server **54** (FIG. **3**) When the user decides to transact business with the Internet Entity it activates an appropriate key which signals a "buy" authorization. This invokes the tracking and authentication module **50** by inputting the second data set to the data base **52** (FIG. **3**). The Internet Entity in response to a "buy" order submits the framed IP address to the certification server **54** (FIG. **2**) which contains the authorized listing of Internet Entities. The Internet Entity server **56** (FIG. **3**) has input the user's encrypted framed IP address which is transmitted to the certification server **54**. The certification server **54** in response to a "buy" order requires the Internet Entity **56** to send its request message **26** (FIG. **2**) encrypted with a key identifying itself. The certification server **54** validates the authenticity of the Internet Entity **28** (FIG. **2**). If validated, the user's first data set coupled with the newly issued framed IP address, the second data set, will identify the user by reading data base table 200, Appendix A-1: 37–41. With the appropriate identification of the user's framed IP address, the certification server **54** (FIG. **3**) sends a message **30** (FIG. **2**) to the database tables to read the Confidential Information by using the first data set with the database tables Appendix A-3: 2–16, 22–45. Unless the user's Confidential Information appropriately qualifies to meet completing the transaction, the tracking and authentication module **50** will generate an error signal **32** denying the transaction. The protected information in the database **52** (FIG. **3**) necessary to complete the transaction is validated **34** (FIG. **2**) to the extent that it is tied to the user. It will not be disclosed outside the data base unless special provision is made to release it. The option is available in certain special circumstances to send the Confidential Information to the Internet Entity. Once the user's credit standing is confirmed the transaction is validated to the Internet Entity **26** so it can be completed.

Referring to FIG. **4** there is shown the look-up tables and data base part of the tracking and authentication module. Starting with the session table 300 the session ID is corroborated with the user ID along with the log-in time. The next table 200, Appendix A-1: 36–37, deals with the framed IP address in which user ID exists only for the current log-in session. Access to the additional information, the user table 400 is conditioned based on the entries in table 200, namely the framed IP address and user ID being matched. The user table 400 provides the essential Confidential Information necessary for completing the transaction, namely assuring the Internet Entity **56** receives payment. It will be understood that the table 300 merely creates a retrievable record of the data entries and generally does not participate in the validation process.

The user table 400 contains addressability information of the user, such as one or more unexpired credit card numbers, credit limits, driver's license information, credit rating as a function of the billing amount. If a run through of the information for the current buy order input to the data base is corroborated with the framed IP address, the user ID, the session ID, the password and other financial benchmarks, an instruction is sent to the Internet Entity that the transaction is validated. Once cleared the data base instructs the ISP to submit the charge under the user's credit card directly to the credit card company who pays the Internet Entity.

In practice, after browsing through a particular home page of an Internet Entity the user will execute a "buy" order **24** (FIG. **1**) activating an appropriate computer key. Once the "buy" order is executed the Internet Entity **56** (FIG. **3**) submits the charge order against the framed IP address to the certification server **54**. It is put through a validation check and if it matches the new user ID, the log-in time, the buy order clearance is communicated to the data base **52**. The clearance is input to the session table 300, Appendix A-2: 112–123 and Appendix A-1: 17–28.

An alternative form of consummating the transaction provides that the data base **52** instruct the certification server **54** of the clearance accompanied by instructions and information that permits the Internet Entity to send a bill directly to the user.

The tracking and authentication module **50** provides for an alternate security control that monitors and tracks the destination address of the user as he browses the available destination Internet Entities for the kinds of goods or services he may be interested in. The table 200, Appendix A-1: 37–44, in addition to the framed IP address includes the destination address which is monitored by the tracking and authentication module **50**. As the user contacts different Internet Entities **56** the POP generates a new destination address which replaces the previous destination address in table 200 forming the referential address. With the additional security control the data base **52** is now programmed to validate a transaction subject the referential address in the date base.

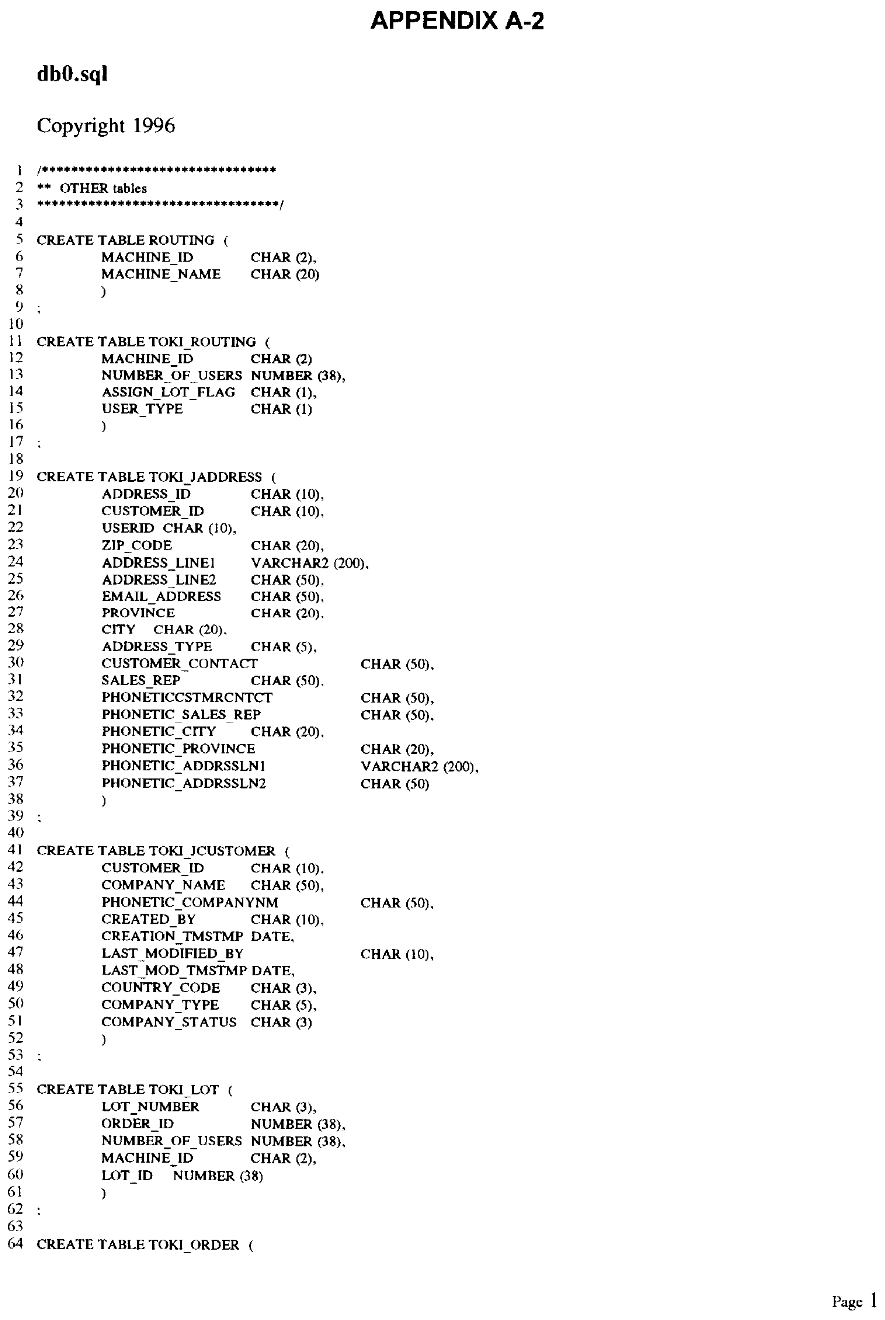
APPENDIX A-1

cr_aws.sql

```
CREATE TABLE AWS_ACCOUNT   (
   USERID CHAR (10)    NOT NULL,
   PURCHASE_STATUS CHAR (1)    NOT NULL,
   USED_AMOUNT NUMBER (10,2)    NOT NULL,
   CREDIT_LINE NUMBER (10,2)    NOT NULL,
   LAST_MOD_TMSTMP  DATE    NOT NULL
   )
   TABLESPACE TOKI_USER_TABLE
;

CREATE INDEX ZABOW05_ZABOZ05  ON AWS_ACCOUNT  (
   USERID
   )
   tablespace  TOKI_USER_INDEX
;

CREATE TABLE AWS_EVENT  (
   USERID CHAR (10)    NOT NULL,
   MERCHANT_ID NUMBER (38)    NOT NULL,
   AWS_EVENT_STATUS CHAR (1)    NOT NULL,
   MERCHANG_ISP_ID  CHAR (10)    NOT NULL,
   MERCH_RQST_CD  CHAR (10)    NOT NULL,
   MERCH_RQST_AMT  NUMBER (10,2)    NOT NULL,
   EVENT_TIMESTAMP DATE    NOT NULL,
   AWS_EVENT_ID  NUMBER (38)    NOT NULL
   )
   tablespace TOKI_SESSION_TABLE
;

CREATE INDEX ZABOB05_ZABQB05  ON AWS_EVENT  (
   AWS_EVENT_ID
   )
   tablespace TOKI_SESSION_INDEX
;

CREATE TABLE AWS_IP_ADDRESS  (
   FRAMED_ADDRESS CHAR (15)    NOT NULL,
   ISP_IP_ADDRESS CHAR (15)    NOT NULL,
   ACCT_SESSION_ID CHAR (16)    NULL,
   NAS_IDENTIFIER CHAR (15)     NULL,
   USERID CHAR (10)  NULL,
   LOGIN_DATE  DATE  NULL,
   ISP_ID CHAR (10)  NOT NULL,
   TARGET_IP_ADDRESS  CHAR (15)  NULL
   )
   tablespace TOKI_OTHER_TABLES
;

CREATE INDEX ZABON05_ZABOT05  ON AWS_IP_ADDRESS  (
   FRAMED_ADDRESS
   )
   tablespace TOKI_OTHER_INDEXES
;

CREATE TABLE AWS_MERCHANT  (
   MERCHANT_ID NUMBER (38)  NOT NULL,
   MERCHANT_NAME CHAR (40)  NOT NULL,
   MERCHANT_ISP_ID CHAR (10)  NOT NULL,
   MERCHANT_PASSWORD CHAR (10)  NOT NULL
   )
   tablespace TOKI_OTHER_TABLES
;

CREATE INDEX ZABOG05_ZABOK05  ON AWS_MERCHANT  (
```

Appendix A-1 (continued)

```
   MERCHANT_ID,
   MERCHANT_ISP_ID
   )
   tablespace TOKI_OTHER_INDEXES
;

/*******************************
* Sequences
*********************************/
create sequence aws_event_id_seq
         increment by 1
         start with 100
         maxvalue 1e+19
         minvalue1
         cache 20
;

/*********************************
* Inserting default values
**********************************/

/** AWS_IP_ADDRESS **/
insert into AWS_IP_ADDRESS
   (FRAMED_ADDRESS, ISP_IP_ADDRESS, ISP_ID)
values ('206.1.167.200', '206.1.167.24', 'AWS-ISP');
insert into AWS_IP_ADDRESS
   (FRAMED_ADDRESS, ISP_IP_ADDRESS, ISP_ID)
values ('206.1.167.201', '206.1.167.24', 'AWS-ISP');

/** AWS_MERCHANT **/
insert into AWS_MERCHANT
   (MERCHANT_ID, MERCHANT_NAME, MERCHANT_ISP_ID, MERCHANT_PASSWORD)
values (1001, 'Sony', 'SNY', 'NOPasswd');
insert into AWS_MERCHANT
   (MERCHANT_ID, MERCHANT_NAME, MERCHANT_ISP_ID, MERCHANT_PASSWORD)
values (1002, 'Philips', "PHLPS', 'NOPsswd');

commit;
exit;
```



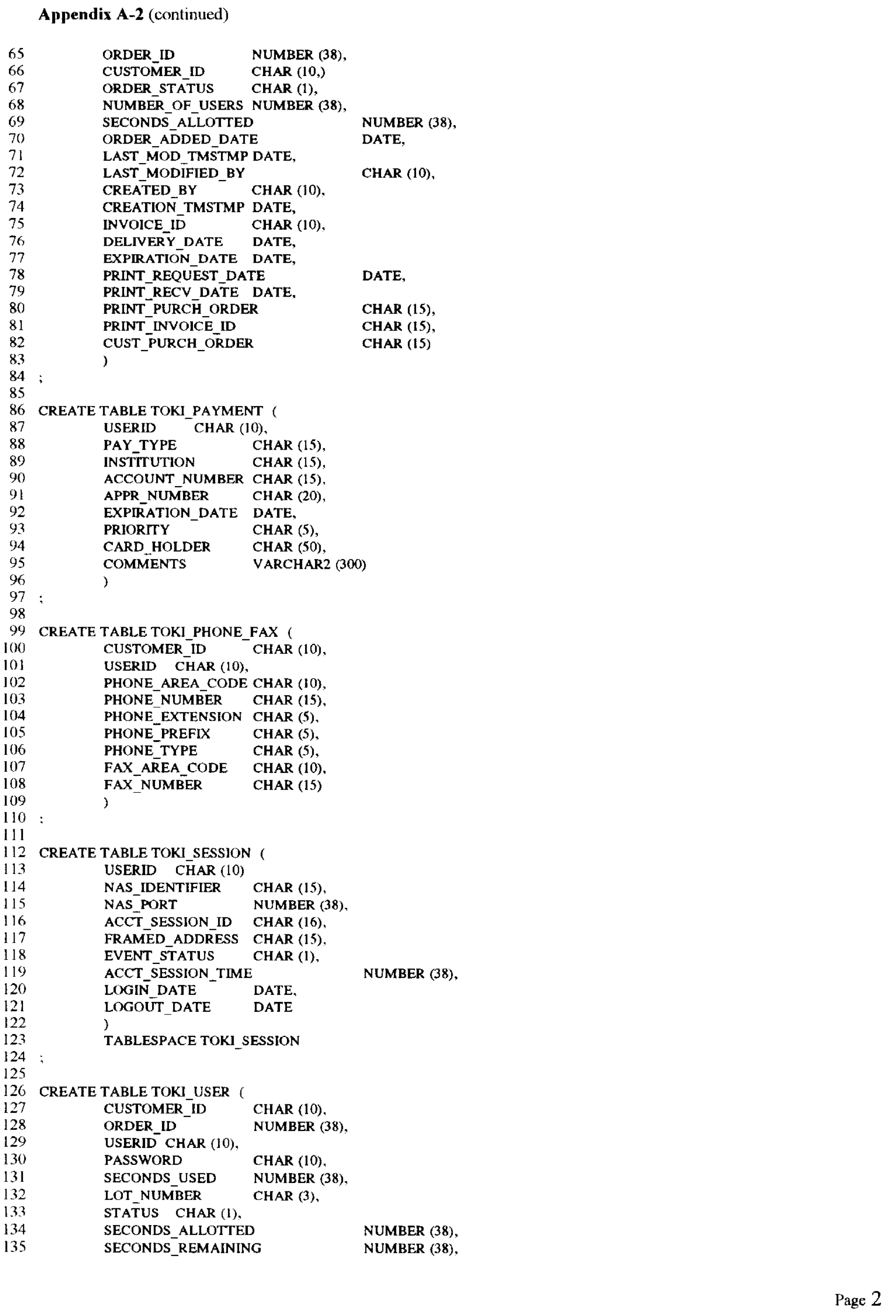
APPENDIX A-2

db0.sql

Copyright 1996

```
/*********************************
** OTHER tables
*********************************/

CREATE TABLE ROUTING (
          MACHINE_ID          CHAR (2),
          MACHINE_NAME        CHAR (20)
          )
;

CREATE TABLE TOKI_ROUTING (
          MACHINE_ID          CHAR (2)
          NUMBER_OF_USERS  NUMBER (38),
          ASSIGN_LOT_FLAG   CHAR (1),
          USER_TYPE           CHAR (1)
          )
;

CREATE TABLE TOKI_JADDRESS (
          ADDRESS_ID          CHAR (10),
          CUSTOMER_ID         CHAR (10),
          USERID  CHAR (10),
          ZIP_CODE            CHAR (20),
          ADDRESS_LINE1       VARCHAR2 (200),
          ADDRESS_LINE2       CHAR (50),
          EMAIL_ADDRESS       CHAR (50),
          PROVINCE            CHAR (20),
          CITY    CHAR (20),
          ADDRESS_TYPE        CHAR (5),
          CUSTOMER_CONTACT                 CHAR (50),
          SALES_REP           CHAR (50),
          PHONETICCSTMRCNTCT               CHAR (50),
          PHONETIC_SALES_REP               CHAR (50),
          PHONETIC_CITY       CHAR (20),
          PHONETIC_PROVINCE                CHAR (20),
          PHONETIC_ADDRSSLN1               VARCHAR2 (200),
          PHONETIC_ADDRSSLN2               CHAR (50)
          )
;

CREATE TABLE TOKI_JCUSTOMER (
          CUSTOMER_ID         CHAR (10),
          COMPANY_NAME        CHAR (50),
          PHONETIC_COMPANYNM               CHAR (50),
          CREATED_BY          CHAR (10),
          CREATION_TMSTMP  DATE,
          LAST_MODIFIED_BY                 CHAR (10),
          LAST_MOD_TMSTMP DATE,
          COUNTRY_CODE        CHAR (3),
          COMPANY_TYPE        CHAR (5),
          COMPANY_STATUS      CHAR (3)
          )
;

CREATE TABLE TOKI_LOT (
          LOT_NUMBER          CHAR (3),
          ORDER_ID            NUMBER (38),
          NUMBER_OF_USERS  NUMBER (38),
          MACHINE_ID          CHAR (2),
          LOT_ID    NUMBER (38)
          )
;

CREATE TABLE TOKI_ORDER (
```

Page 1



Appendix A-2 (continued)

```
        ORDER_ID            NUMBER (38),
        CUSTOMER_ID         CHAR (10,)
        ORDER_STATUS        CHAR (1),
        NUMBER_OF_USERS     NUMBER (38),
        SECONDS_ALLOTTED                    NUMBER (38),
        ORDER_ADDED_DATE                    DATE,
        LAST_MOD_TMSTMP     DATE,
        LAST_MODIFIED_BY                    CHAR (10),
        CREATED_BY          CHAR (10),
        CREATION_TMSTMP     DATE,
        INVOICE_ID          CHAR (10),
        DELIVERY_DATE       DATE,
        EXPIRATION_DATE     DATE,
        PRINT_REQUEST_DATE                  DATE,
        PRINT_RECV_DATE     DATE,
        PRINT_PURCH_ORDER                   CHAR (15),
        PRINT_INVOICE_ID                    CHAR (15),
        CUST_PURCH_ORDER                    CHAR (15)
        )
;

CREATE TABLE TOKI_PAYMENT (
        USERID      CHAR (10),
        PAY_TYPE            CHAR (15),
        INSTITUTION         CHAR (15),
        ACCOUNT_NUMBER      CHAR (15),
        APPR_NUMBER         CHAR (20),
        EXPIRATION_DATE     DATE,
        PRIORITY            CHAR (5),
        CARD_HOLDER         CHAR (50),
        COMMENTS            VARCHAR2 (300)
        )
;

CREATE TABLE TOKI_PHONE_FAX (
        CUSTOMER_ID         CHAR (10),
        USERID    CHAR (10),
        PHONE_AREA_CODE     CHAR (10),
        PHONE_NUMBER        CHAR (15),
        PHONE_EXTENSION     CHAR (5),
        PHONE_PREFIX        CHAR (5),
        PHONE_TYPE          CHAR (5),
        FAX_AREA_CODE       CHAR (10),
        FAX_NUMBER          CHAR (15)
        )
;

CREATE TABLE TOKI_SESSION (
        USERID    CHAR (10)
        NAS_IDENTIFIER      CHAR (15),
        NAS_PORT            NUMBER (38),
        ACCT_SESSION_ID     CHAR (16),
        FRAMED_ADDRESS      CHAR (15),
        EVENT_STATUS        CHAR (1),
        ACCT_SESSION_TIME                   NUMBER (38),
        LOGIN_DATE          DATE,
        LOGOUT_DATE         DATE
        )
        TABLESPACE TOKI_SESSION
;

CREATE TABLE TOKI_USER (
        CUSTOMER_ID         CHAR (10),
        ORDER_ID            NUMBER (38),
        USERID  CHAR (10),
        PASSWORD            CHAR (10),
        SECONDS_USED        NUMBER (38),
        LOT_NUMBER          CHAR (3),
        STATUS    CHAR (1),
        SECONDS_ALLOTTED                    NUMBER (38),
        SECONDS_REMAINING                   NUMBER (38),
```

Appendix A-2 (continued)

```
        LAST_LOGIN_TMSTMP                 DATE,
        LAST_LOGOUT_TMSTMP                DATE,
        COUNTRY_CODE      CHAR (3),
        CREATED_BY        CHAR (10),
        CREATION_TMSTMP  DATE,
        LAST_MODIFIED_BY                  CHAR (10),
        LAST_MOD_TMSTMP DATE
        )
        TABLESPACE TOKI_USER_TABLE
;

/****
***   INDEX
***/

CREATE  INDEX TOKI_JADDRESS_I1  ON
        TOKI_JADDRESS  (ADDRESS_ID)
;

CREATE INDEX TOKI_JCUSTOMER_I1  ON
        TOKI_JCUSTOMER  (CUSTOMER_ID)

CREATE INDEX TOKI_LOT_I1  ON
        TOKI_LOT  (LOT_ID)
;

CREATE INDEX TOKI_ORDER_I1  ON
        TOKI_ORDER  (ORDER_ID)
;

CREATE INDEX TOKI_PAYMENT_I1  ON
        TOKI_PAYMENT (USERID, DBID_TOKI_PAYMENT)
;

CREATE INDEX TOKI_PHONE_FAX_I1  ON
        TOKI_PHONE_FAX  (PHONE_ID)
;

CREATE INDEX TOKI_SESSION_I1  ON
        TOKI_SESSION (ACCT_SESSION_ID, USERID, NAS_IDENTIFIER)
        TABLESPACE TOKI_USER_INDEX
;

CREATE INDEX TOKI_USER_I1  ON
        TOKI_USER (USERID)
        TABLESPACE TOKI_USER_INDEX
;

CREATE TABLE TOKI_SECURITY  (
        SYSTEM_GROUP_ID  CHAR (10),
        PROCESS_ID          CHAR (40)
        )
;

CREATE TABLE TOKI_SYSTEM_USER  (
        SYSTEM_USERID      CHAR (10),
        SYSTEM_GROUP_ID  CHAR (10),
        PASSWORD            CHAR (10)
        )
;

CREATE INDEX TOKI_SECURITY_I1  ON
        TOKI_SECURITY (SYSTEM_GROUP_ID, PROCESS_ID)
;

CREATE INDEX TOKI_SYSTEM_USER_I1  ON
        TOKI_SYSTEM_USER (SYSTEM_USERID)
;
```

APPENDIX A-3

db0.sql

```
CREATE TABLE TOKI_IND_USER (
        USERID    CHAR (10),
        PASSWORD            CHAR (10),
        BILL_TO   CHAR (10),
        SERVICE_TYPE        CHAR (15),
        SECONDS_USED        NUMBER (38),
        LAST_LOGIN_TMSTMP                   DATE,
        LAST_LOGOUT_TMSTMP                  DATE,
        SECONDS_MAX         NUMBER (38),
        COUNTRY_CODE        CHAR (3),
        BELONG_TO           CHAR (10),
        STATUS      CHAR (1),
        CREATED_BY          CHAR (10),
        CREATION_TMSTMP DATE,
        LAST_MODIFIED_BY                    CHAR (10),
        LAST_MOD_TMSTMP DATE
        )
        TABLESPACE TOKI_USER_TABLE
;

CREATE TABLE TOKI_IND_USER_INFO (
        USER_PHON_FIRST_NM                  CHAR (50),
        USER_PHON_LAST_NM                   CHAR (50),
        USER_LAST_NM        CHAR (50),
        USER_FIRST_NM       CHAR (50),
        USERID      CHAR (10),
        USER_ENGL_FIRST_NM                  CHAR (50),
        USER_ENGL_LAST_NM                   CHAR (50),
        BIRTHDATE           DATE,
        OCCUPATION          CHAR (50),
        EMAIL_ADDRESS1      CHAR (50),
        EMAIL_ADDRESS2      CHAR (50),
        EMAIL_ADDRESS3      CHAR (50),
        EMAIL_PASSWORD1     CHAR (10),
        EMAIL_PASSWORD2     CHAR (10),
        EMAIL_PASSWORD3     CHAR (10),
        GARD_FIRST_NM       CHAR (50),
        GARD_PHON_FIRST_NM                  CHAR (50),
        GARD_ENGL_FIRST_NM                  CHAR (50),
        GARD_PHON_LAST_NM                   CHAR (50),
        GARD_LAST_NM        CHAR (50),
        GARD_ENGL_LAST_NM                   CHAR (50),
        SEX       CHAR (1),
        COMPANY_NAME        CHAR (50),
        COMMENTS            VARCHAR2 (300)
        )
        TABLESPACE TOKI_USER_TABLE
;

CREATE INDEX TOKI_IND_USER_I1  ON
        TOKI_IND_USER (USERID)
        TABLESPACE TOKI_USER_INDEX
;

/**
**  SEQUENCE
**/

CREATE SEQUENCE ADDRESS_ID_SEQ
        INCREMENT BY 1
        START WITH 100
        MAXVALUE 1e+19
        MINVALUE 1
        CACHE 30
```

Appendix A-3 (continued)

```
;
CREATE SEQUENCE CUSTOMER_ID_SEQ
          INCREMENT BY 1
          START WITH 100
          MAXVALUE 1e+19
          MINVALUE 1
          CACHE 30
;
CREATE SEQUENCE KANJI_ID_SEQ
          INCREMENT BY 1
          START WITH 100
          MAXVALUE 1e+19
          MINVALUE 1
          CACHE 30
;
CREATE SEQUENCE LOT_NUMBER_SEQ
          INCREMENT BY 1
          START WITH 100
          MAXVALUE 1e+27
          MINVALUE 1
          CACHE 20
;
CREATE SEQUENCE ORDER_ID_SEQ
          INCREMENT BY 1
          START WITH 100
          MAXVALUE 1e+19
          MINVALUE 1
          CACHE 30
;
CREATE SEQUENCE PHONE_ID_SEQ
          INCREMENT BY 1
          START WITH 100
          MAXVALUE 1e+19
          MINVALUE 1
          CACHE 30
;
CREATE SEQUENCE SESSION_ID_SEQ
          INCREMENT BY 1
          START WITH 100
          MAXVALUE 1e+19
          MINVALUE 1
          CACHE 30
;
CREATE SEQUENCE TOKI_PAYMENT_ID_SEQ
          INCREMENT BY 1
          START WITH 100
          MAXVALUE 1e+19
          MINVALUE 1
          CACHE 30
;
CREATE SEQUENCE TOKI_SEED_SEQ
          INCREMENT BY 1
          START WITH 100
          MAXVALUE 1e+27
          MINVALUE 1
          CACHE 20
```

Although the invention has been described with particular reference to certain preferred embodiments thereof, variations and modifications can be effected with the spirit and scope of the following claims.

What is claimed is:

1. A method of authenticating a user's confidential information and preserving the confidentiality against unauthorized use, said information being essential for conducting Internet transactions between a log-in and log-out session, comprising the steps of:

accessing the Internet by the user entering a first data set into a computer based controller to control modems and communication protocols;

establishing a data base containing confidential information subject to authentication with a user's first data set;

submitting said first data set to a tracking and authentication control module requesting authentication of the user, said tracking and authentication control module including a data base containing user's confidential information, an authentication server for authenticating said first data set and a certification server, said certification server containing validation data for authenticating and internet entity approved for conducting internet transaction;

comparing the user's first data set input to the authentication server incident to accessing the internet with the I.D. and password in the data base and subject to a validating match;

issuing a second data set in real time by the authentication server subject to a validation match of the I.D. and password with the data in the database usable for the instant transaction;

submitting the second data set to the certification server upon the initiation of a transaction by the user;

consummating the transaction subject to validation of the second data set by tying the confidential information in the data base to the user whereby the confidential information is retained undisclosed in the data base.

2. The method as claimed in claim **1** wherein the second data set is a framed-IP-address.

3. The method as claimed in claim **1** wherein the framed -IP- address is confirmed by the data base and the authorization control module certifies the credit standing of the user.

4. The method as claimed in claim **1** wherein the user initiates an Internet transaction by inputting the second data set to the Internet Entity and said Internet Entity queries the certification server to verify the identity of the second data set as a condition of completing the transaction.

5. The method as claimed in claim **1** wherein the data base comprises a series of look-up tables containing the first data set, the second data set and the confidential information.

6. The method as claimed in claim **5** wherein the tables in the data base are updated in real time keeping track of each transaction.

7. A method of controlling a user's confidential information and preserving the confidentiality against unauthorized use, said information being essential for conducting internet transactions between a log-in and log-out session, comprising the steps of:

accessing the internet by the user entering a first data set into a computer based controller to control modems and communication protocols;

establishing a data base containing user's confidential information subject to authentication with a user's first data set;

submitting said first data set to an authentication control module requesting authentication of the user, said authentication control module including a data base containing user's confidential information, and authentication server containing validation data for authenticating an internet entity approved for conducting Internet transactions; comparing the user's first data set incident to accessing the internet with the confidential information in the data base and subject to a validating match said computer based controller for controlling modems and communication protocols issuing a second data set;

monitoring the user's selection of an internet entity by the tracking and authentication module and the authentication server and wherein the POP issues a third data set, said second data set and third data set being issued in real time usable for the internet log-in transaction; and

consummating a transaction subject to the authentication of the second and third data sets with the first data set in the data base thereby tying the confidential information to the user whereby the confidential information is retained undisclosed in the data base.

8. The method as claimed in claim **7** wherein the third data set is the destination address of the internet entity browsed or engaged by the user.

9. The method as claimed in claim **7** wherein computer based controller for controlling modems and communication protocols is a point of presence program.

10. The method as claimed in claim **7** wherein the certification server identifies the Internet Entity as authorized to conduct transactions on the Internet.

11. The method as claimed in claim **7** wherein the authentication control module tracks the Internet Entity browsed or engaged by the user during the session updating the data base and issuing a new third data set with each such browsing or engagement contact.

12. The method as claimed in claims **1** and **7** wherein the data base can alternately authorizes the certification module to instruct the Internet Entity to bill any charges directly to the user.

13. A method of controlling the confidentiality of a user's Confidential information against unauthorized use, said information being essential for conducting internet transactions comprising the steps of:

providing a data base for tracking and authenticating information input to a tracking and authentication module, said tracking and authentication module including an authentication server and certification server;

establishing a series of look up tables in said data base that record the i.d. and password of the user, the framed IP address, destination IP address and the user's confidential information, said tables including a user table containing the addressability information of the user;

submitting a first data set into the tracking and authentication module;

performing a validation check of the user's first data set with the confidential information in said user table;

issuing a second data set responsive to a successful validation of the first data set with the information in the series of tables;

inputting in real time the second data set to the look up tables;

consummating a transaction subject to the authentication of the second data set with the information in the user table confirming the user as the owner of the confidential information, whereby the confidential information is maintained undisclosed in a series of look up tables.

* * * * *